RISK ASSESSMENT PLANNING FOR AIRBORNE SYSTEMS: AN INFORMATION ASSURANCE FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS METHODOLOGY

GRADUATE RESEARCH PAPER

Charles J. Middleton, Major, USAF
AFIT/IOA/ENS/12-05

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/IOA/ENS/12-05

RISK ASSESSMENT PLANNING FOR AIRBORNE SYSTEMS: AN INFORMATION ASSURANCE FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS METHODOLOGY

GRADUATE RESEARCH PAPER

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Analysis

Charles J. Middleton, BSE

Major, USAF

June 2012

AFIT/IOA/ENS/12-05

RISK ASSESSMENT PLANNING FOR AIRBORNE SYSTEMS: AN INFORMATION ASSURANCE FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS METHODOLOGY

Charles J. Middleton, BSE
Major, USAF

Approved:

_____	_____
Dr. Raymond Hill (Chairman)	Date

Abstract

Increasingly in recent times, aircraft are built with communications links to external participants. These communications links may in some cases be susceptible to degradation or attack, which may then lead to safety of flight or mission effectiveness risks. This project examines risk assessment of the information assurance and security of newly developed airborne systems. First, an investigation of the past failures of the security of other networked systems is examined, to give a historical perspective on the likely scope of system security threats and vulnerabilities. Next, risk assessment methods are summarized for current methods of analyzing risk to aircraft and other systems. An information assurance Failure Mode, Effects and Criticality Analysis (FMECA) methodology is presented, based on past FMECA methodologies with modifications tailored to aircraft systems and the information warfare environment, to examine the system integrity considerations in planning for the development of new military aircraft. A program manager's potential decisions are informed with insights on failure mode risk criticality, based on the information assurance FMECA method. Finally, recommendations for follow-on research in the airborne systems information assurance field are detailed.

Table of Contents

List of Figures

List of Tables

RISK ASSESSMENT PLANNING FOR AIRBORNE SYSTEMS: AN INFORMATION ASSURANCE FAILURE MODE, EFFECTS AND CRITICALITY ANALYSIS METHODOLOGY

I. Introduction

Background

Aircraft in the twenty-first century are amazingly complex machines built with increasingly many types of electronic subsystems. These systems are often interconnected to external participants through radio frequencies, datalinks, satellite links, or other communication means. While the information sharing between systems provided by the continuous advance of technology allows aircraft new capabilities and efficiencies that were unreachable in the past, these same technologies provide vulnerabilities through which an aircraft can be attacked.

Information system assurance is a critically important requirement not only for the typical information systems we use every day, such as banking, finance, industry, entertainment, shopping and social networking, but also for airborne systems. Military aircraft need special attention in the information assurance realm as the benefits of a successful attack on a military aircraft provide benefits to a wide range of potential adversaries.

To date, little has been published on the specific requirements of airborne systems for information assurance. Program managers and airworthiness certification authorities are grappling with the challenges of how to ensure that new aircraft have systems which are secure from electronic warfare threats. This paper examines risk assessment planning for airborne systems, by proposing a methodology for failure mode, effects and criticality

analysis which applies to information assurance of those systems. The methodology draws on prior risk analysis of failure modes in other fields, and integrates unique challenges of the information assurance environment.

Problem Statement

The problem this research addresses is the assessment of information assurance risks to airborne systems by program managers and certification authorities.

Research Objectives

This research effort has the primary objective of providing a methodology which systematically analyzes information assurance risks to airborne systems. The following sub-objectives support this primary objective:

- Provide clear metrics for measuring risk factors,
- Provide a framework for understanding the criticality of risks,
- Incorporate a mitigation plan into the risk analysis process, and
- Provide insight to program managers and certification authorities on the risk criticality of failure modes and the factors involved.

II. Literature Review

Overview

Before offering potential solutions to the problem of information assurance for airborne systems, we will clarify the existence of a problem and characterize the nature of the challenges the problem presents. To this end, we review briefly past literature on the information assurance problem as it has applied in the past, primarily for networked computer systems. We review the basics of information assurance from the Department of Defense's perspective. Then we present a variety of recent articles on information assurance failures from across a range of systems, to include some airborne systems.

Next, we summarize the potential challenges of information assurance for airborne systems and some unique characteristics of information warfare. Then we move into the methods others have used in the past to study and understand complex systems and their vulnerabilities. Finally we look at failure mode, effects, and criticality analysis (FMECA) as presented by past authors and show some of the applications of FMECA in other systems environments.

Background and Motivation

Information assurance is defined by the Department of Defense in Joint Publication 3-13 (Joint Warfighting Center, 2006) as the foremost supporting principle of defensive information operations (IO). Specifically,

> **"Information assurance"** is defined as measures that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Each of the characteristics of information assurance is also defined by the Joint Pub (Figure 1). Availability is defined as assured access by authorized users. Confidentiality

is defined as protection from unauthorized disclosure. Integrity is defined as protection from unauthorized change. Together these help ensure the necessary protection and defense of information and information systems.

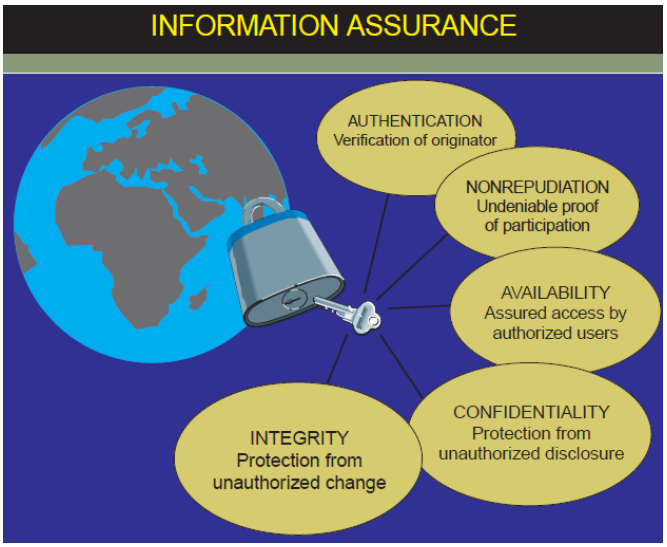


Figure 1: Information Assurance Characteristics

With the emergence of cyberspace as an additional domain in which conflict can occur, the threats to information systems has grown vastly over the past 15 years. The importance of our information systems and the potentially disruptive challenges of protecting it may alter fundamentally the long-established concepts of warfare (Alexander, 2007). Indeed, dominance of cyberspace, along with dominance of air and space, provide the high ground for freedom of action in military operations of the future (Lambeth, 2011). The defense of friendly systems that is gained by information assurance is critical for the future success of military operations.

Unfortunately, providing information assurance for networked systems has proved immensely difficult for system engineers. This is evident by the multitude of

information attacks on all types of information systems worldwide, including those used by the military, other government agencies, civilian institutions, and private commercial systems. We now examine several instances of the failure of a system to ensure availability, confidentiality, or integrity. These examples come from all types of systems, not just military ones. Sources for these article excerpts can be found in the bibliography.

MasterCard and Visa Investigate Data Breach
March 30, 2012
Visa and MasterCard are investigating whether a data security breach at one of the main companies that processes transactions improperly exposed private customer information, bank officials said Friday. The event highlighted a crucial vulnerability that could affect millions of credit card holders.
The breach occurred at Global Payments, an Atlanta company that helps Visa and MasterCard process transactions for merchants. One bank executive estimated that about one million to three million accounts could be affected. That does not mean that all those cards were used fraudulently, but that credit card information on the cardholders was exposed.

Sony Says PlayStation Hacker Got Personal Data
April 26, 2011
Last week, Sony's online network for the PlayStation suffered a catastrophic failure through a hacking attack. And since then, the roughly 77 million gamers worldwide like Mr. Miller who have accounts for the service have been unable to play games with friends through the Internet or to download demos of new games. Then, on Tuesday, after several days of near silence, Sony said that as a result of the attack, an "unauthorized person" had obtained personal information about account holders, including their names, addresses, e-mail addresses, and PlayStation user names and passwords. Sony warned that other confidential information, including credit card numbers, could have been compromised, warning customers through a statement to "remain vigilant" by monitoring identity theft or other financial loss.

Slammer worm crashed Ohio nuke plant network
August 19, 2003
The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned. The breach did not pose a safety hazard. The troubled plant had been offline since February, 2002, when workers discovered a 6-by-5-inch hole in the plant's reactor head. Moreover, the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm. But at least one expert says the case illustrates a growing cybersecurity problem in the nuclear power industry, where interconnection between plant and corporate networks is becoming more common, and is permitted by federal safety regulations.

America's Hackable Backbone
August 22, 2007
The first time Scott Lunsford offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for IBM's Internet Security Systems, found otherwise. "It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a big problem.'" In retrospect, Lunsford says--and the Nuclear Regulatory Commission agrees--that government-mandated safeguards would have prevented him from triggering a nuclear meltdown. But he's fairly certain that by accessing controls through the company's network, he could have sabotaged the

power supply to a large portion of the state. "It would have been as simple as closing a valve," he says.

$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected

December 17, 2009

Militants in Iraq have used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, potentially providing them with information they need to evade or monitor U.S. military operations. Senior defense and intelligence officials said Iranian-backed insurgents intercepted the video feeds by taking advantage of an unprotected communications link in some of the remotely flown planes' systems. Shiite fighters in Iraq used software programs such as SkyGrabber -- available for as little as $25.95 on the Internet -- to regularly capture drone video feeds, according to a person familiar with reports on the matter. The Air Force has staked its future on unmanned aerial vehicles. Drones account for 36% of the planes in the service's proposed 2010 budget.

Computer Virus Hits U.S. Drone Fleet

October 7, 2011

A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones. The virus, first detected nearly two weeks ago by the military's Host-Based Security System, has not prevented pilots at Creech Air Force Base in Nevada from flying their missions overseas. Nor have there been any confirmed incidents of classified information being lost or sent to an outside source. But the virus has resisted multiple efforts to remove it from Creech's computers, network security specialists say. And the infection underscores the ongoing security risks in what has become the U.S. military's most important weapons system. "We keep wiping it off, and it keeps coming back," says a source familiar with the network infection, one of three that told Danger Room about the virus. "We think it's benign. But we just don't know." Military network security specialists aren't sure whether the virus and its so-called "keylogger" payload were introduced intentionally or by accident; it may be a common piece of malware that just happened to make its way into these sensitive networks. The specialists don't know exactly how far the virus has spread. But they're sure that the infection has hit both classified and unclassified machines at Creech. That raises the possibility, at least, that secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

SkyNet Satellite Hacked

May 8, 2007

Computer hackers have reportedly gained control of the British SkyNet military communications satellite which has triggered a "frenetic" security alert, says the UK's Daily Telegraph. The hackers have been traced to the south of England. A security source said hackers found a "cute way" into the control system for one of the Ministry of Defence's Skynet satellites, up to a month ago, and "changed the characteristics of channels used to convey military communications, satellite television and telephone calls". The hackers intercepted the link between the Skynet's control center and the ground station. The source said the hackers "managed to reprogram a satellite control system. In many ways, the clever thing was not to lose the satellite."

'We hacked U.S. drone'
December 15, 2011
An Iranian engineer today claimed how his country managed to 'trick' a US. drone into landing in Iran by electronically hacking into its navigational weak spot and 'spoofing' its GPS system.
It's the latest development in this extraordinary tale of intrigue, with a Christian Science Monitor report citing a 2003 document suggesting the GPS weakness was long known to the U.S. military. The RQ-170 Sentinel has been seen on display by Iran's gloating military after it went missing along the Afghan-Iran border earlier this month - but a former Pentagon official said it seems to be a fake.

Stuxnet virus targets and spread revealed
February 15, 2011
A powerful internet worm repeatedly targeted five industrial facilities in Iran over 10 months, ongoing analysis by security researchers shows. Stuxnet, which came to light in 2010, was the first-known virus specifically designed to target real-world infrastructure, such as power stations. Security firm Symantec has now revealed how waves of new variants were launched at Iranian industrial facilities. Some versions struck their targets within 12 hours of being written.

"We are trying to do some epidemiology," Orla Cox of Symantec told BBC News. "We are trying to understand how and why it spread." The worm first grabbed headlines late last year after initial analysis showed that the sophisticated piece of malware had likely been written by a "nation state" to target Iran's nuclear programme, including the uranium enrichment centrifuges at the Natanz facility. Russia's Nato ambassador recently said the virus "could lead to a new Chernobyl," referring to the 1986 nuclear accident. Although speculation surrounds which countries may have been involved in its creation, the origins of the worm still remain a mystery. Iranian officials have admitted that the worm infected staff computers. However, they have repeatedly denied that the virus caused any major delays to its nuclear power programme, although its uranium enrichment programme is known to have suffered setbacks.

China's hacking skills in spotlight
September 16, 2007
When suspected Chinese hackers penetrated the Pentagon this summer, reports downplayed the cyberattack. The hackers hit a secure Pentagon system known as NIPRNet — but it carries only unclassified information and general e-mail, Department of Defense officials said. Yet a central aim of the Chinese hackers may not have been top secrets, but a probe of the Pentagon network structure itself, some analysts argue. The NIPRNet (Non-classified Internet Protocol Router Network) is crucial in the quick deployment of U.S. forces should China attack Taiwan. By crippling a Pentagon network used to call U.S. forces, China gains crucial hours and minutes in a lightning attack designed to force a Taiwan surrender, experts say.

China's Role In JSF's Spiraling Costs
February 6, 2012
How much of the F-35 Joint Strike Fighter's spiraling cost in recent years can be traced to China's cybertheft of technology and the subsequent need to reduce the fifth-generation aircraft's vulnerability to detection and electronic attack? That is a central question that budget planners are asking, and their queries appear to have validity. Moreover, senior Pentagon and industry officials say other classified weapon programs are suffering from the same problem. Before the intrusions were discovered nearly three years ago, Chinese hackers actually sat in on what were supposed to have been secure, online program-progress conferences, the officials say.

The full extent of the connection is still being assessed, but there is consensus that escalating costs, reduced annual purchases and production stretch-outs are a reflection to some degree of the need for redesign of critical equipment. Examples include specialized communications and antenna arrays for stealth aircraft, as well as significant rewriting of software to protect systems vulnerable to hacking. The F-35 program may have been vulnerable because of its lengthy development. Defense analysts note that the JSF's information system was not designed with cyberespionage, now called advanced persistent threat, in mind. Lockheed Martin officials now admit that subcontractors (6-8 in 2009 alone, according to company officials) were hacked and "totally compromised." In fact, the stealth fighter program probably has the biggest "attack surface" or points that can be attacked owing to the vast number of international subcontractors.

There also is the issue of unintended consequences. The 2009 hacking was apparently not aimed at the F-35 but rather at a classified program. However, those accidental results were spectacular. Not only could intruders extract data, but they became invisible witnesses to online meetings and technical discussions, say veteran U.S. aerospace industry analysts. After the break-in was discovered, the classified program was halted and not restarted until a completely new, costly and cumbersome security system was in place.

FAA's Air-Traffic Networks Breached by Hackers
May 7, 2009
Civilian air-traffic computer networks have been penetrated multiple times in recent years, including an attack that partially shut down air-traffic data systems in Alaska, according to a government report. The report, which was released by the Transportation Department's inspector general Wednesday, warned that the Federal Aviation Administration's modernization efforts are introducing new vulnerabilities that could increase the risk of cyberattacks on air-traffic control systems. The FAA is slated to spend approximately $20 billion to upgrade its air-traffic control system over the next 15 years.

The nature of one 2006 attack is a matter of dispute between the inspector general and the FAA. The report says the attack spread from administration networks to air-traffic control systems, forcing the FAA to shut down a portion of its traffic control systems in Alaska. Ms. Brown said it affected only the local administrative system that provides flight and weather data to pilots, primarily of small aircraft. Last year, hackers of unspecified origin "took over FAA computers in Alaska" to effectively become agency insiders, and traveled the agency networks to Oklahoma, where they stole the network administrator's password and used it to install malicious codes, the report said. These hackers also gained the ability to obtain 40,000 FAA passwords and other information used to control the administrative network, it said.

Hackers Attack Air Traffic Control
August 29, 2011
Britain's Civil Aviation Authority has issued a safety alert about a new threat to air passengers: hackers taking over air traffic control transmissions and giving pilots bogus orders. The number of incidents in which radio hackers have broken into frequencies used by British air traffic controllers and given false instructions to pilots, or broadcasted fake distress calls, are on an alarming rise. There were three such incidents there in 1998, 18 last year, and now, so far this year, 20.

Fortunately in all those cases, pilots ascertained that the directions given them were fake. But had they not done so, their lives and those of their passengers could have been placed in serious jeopardy. The problem is not unique to the U.K. In the United States, there have been fewer reported incidents involving falsified radio transmissions, but the threat is still real. In April of last year, the pilot of a USAir flight approaching Washington's Reagan National Airport was instructed to divert his landing by an unknown voice breaking into his frequency, causing confusion for himself and for two other planes in position to land.

Challenges and Efforts to Secure Control Systems
March 30, 2004
In 1994, the computer system of the Salt River Project, a major water and electricity provider in Phoenix, Arizona, was breached. In March 1997, a teenager in Worcester, Massachusetts, remotely disabled part of the public switching network, disrupting telephone service for 600 residents and the fire department and causing a malfunction at the local airport. In the spring of 2000, a former employee of an Australian company that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely hack into the controls of a sewage treatment system and ultimately release about 264,000 gallons of raw sewage into nearby rivers and parks. In the spring of 2001, hackers mounted an attack on systems that were part of a development network at the California Independent System
Operator, a facility that is integral to the movement of electricity throughout the state.

Is Innovative Aerospace Technology Getting Too Far Ahead of Itself?
June, 2011
The simple failure of a radio altimeter led to the delayed attempts at stall recovery of the Turkish Airlines Boeing 737 Flight 951 in which the investigators' preliminary report confirmed that the pilots allowed the automatic systems to decelerate the aircraft to a dangerously low speed as it approached Schiphol Airport. Very late detection and pilot response at 450 feel AGL; the pilots scrambled to accelerate out of the stall before it crashed to the ground, killing the three flight deck crew and six others on board. The radio altimeter had "informed" the automatic flight system that the aircraft was 8 feet below the surface when it was still nearly 2,000 ft in the air which caused the auto-throttle to pull back the thrust levers to idle, as if the plane were touching down.

Federal Aviation Administration 14 CFR Part 25 [Docket No. NM364 Special Conditions No. 25-356-SC]
January 2, 2008
These special conditions are issued for the Boeing Model 787-8 airplane. This airplane will have novel or unusual design features when compared to the state of technology envisioned in the airworthiness standards for transport category

> airplanes. These novel or unusual design features are associated with connectivity of the passenger domain computer systems to the airplane critical systems and data networks. For these design features, the applicable airworthiness regulations do not contain adequate or appropriate safety standards for protection and security of airplane systems and data networks against unauthorized access.
>
> The proposed architecture of the 787 is different from that of existing production (and retrofitted) airplanes. It allows new kinds of passenger connectivity to previously isolated data networks connected to systems that perform functions required for the safe operation of the airplane. Because of this new passenger connectivity, the proposed data network design and integration may result in security vulnerabilities from intentional or unintentional corruption of data and systems critical to the safety and maintenance of the airplane.
>
> Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Boeing Model 787-8 airplane.
>
> The design shall prevent all inadvertent or malicious changes to, and all adverse impacts upon, all systems, networks, hardware, software, and data in the Aircraft Control Domain and in the Airline
> Information Domain from all points within the Passenger Information and Entertainment Domain.

As seen in this collection of articles, information assurance presents a wide range of challenges to the military, to other government agencies, and to civilian and private industry. From these examples, we gain some insight on the types of threats that might exist to information systems and the types of vulnerabilities and effects that they might cause.

Program managers, engineers and analysts should note the important characteristics of information systems and information assurance as illustrated by the above article excerpts, summarized here as some key concepts of the information assurance, especially for military and airborne systems:

- All types of information systems are vulnerable to attack—civilian, private, military.
- Systems thought to be unassailable for security may be vulnerable.

- When systems are attacked, managers and users may not be immediately aware of the attack.
- Even if aware, system managers' notifications or warnings may not be forthcoming with attack details and effects.
- Critical national infrastructure has been attacked in the past and is vulnerable.
- Military systems have been attacked in the past and are vulnerable.
- Airborne systems including drone and satellites have been attacked and are vulnerable.
- Sources of attack are widely varying, including nation-states, small groups, and individuals.
- For some attacks, attribution of the origin for the attack may be impossible to determine.
- Recently, potential adversary nation-states have attacked US information and airborne systems.
- Modern aircraft now have information systems integrated into their design, which can provide connectivity to systems required for the safe operation of the airplane.
- Delay in detection of an airborne system failure mode may dramatically increase the severity of the failure.

Together, these characteristics of information assurance, and how they relate to airborne systems, create a monumental challenge for design engineers and program managers to grapple with, as the information system threats are widespread, the system

vulnerabilities are numerous and difficult to defend, and the effects of a breach in system assurance can be severe.

An Aircraft as a System of Systems

An aircraft is an especially difficult system to defend against information assurance threats. A military aircraft in today's world is an extremely complex entity composed of subsystems which themselves are extremely complex. These subsystems perform a vast array of functions, from powering the aircraft, to controlling its flight, to navigation, monitoring air traffic, to communicating with other aircraft and with ground personnel, to managing enormous cargo, to providing in-flight refueling of other aircraft, to supporting enormous high-powered radars, lasers, and cameras, to carrying and launching a wide array of missiles and bombs, along with many more functions too. As such, the vulnerabilities and effects that an information assurance failure might have on an aircraft are numerous. Understanding the possible effects of a failure of an aircraft system is in itself a complex field not easy to grasp.

As such, the analysts responsible for risk analysis and mitigation efforts of information system attacks on an aircraft should consider other work on analyzing effects on complex systems. When analyzing the effects of a kinetic attack on a nation-state, the objective of strategic paralysis can be modeled using the Five-Ring theory (Warden, 1995). This analysis takes the view of the attacker attempting to control the strategic center of an enemy system, and works from the big picture of the core functionality of the system, down to outer more detailed layers which support and enable the functionality of the strategic core. For an aircraft system, the mission effectiveness and safety of flight of the aircraft can be considered as corollary to the strategic core of a nation-state. An

enemy attacker, through an information system vulnerability, likely desires not only to degrade or disable an outer support layer of the aircraft's functionality, but also to degrade or disable the core ability of the aircraft and its crew to complete its operational mission. In analyzing threats and vulnerabilities to an aircraft, one must keep in mind that the overall functionality of the aircraft and how well it can perform its assigned mission is the overarching motivation which information assurance must support.

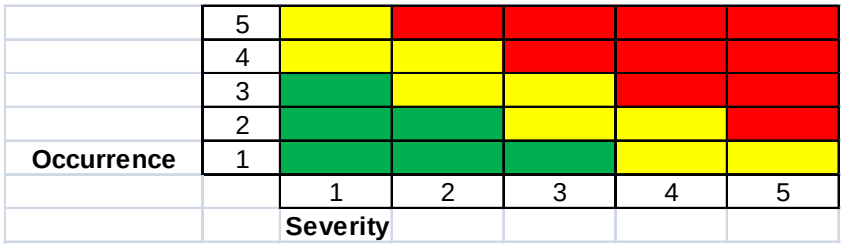
An aircraft, as a highly complex vehicle, can be modeled as a system of systems. System-of-systems analysis (SOSA) is one technique used to model an operational environment, to understand the organization and information of the system, and assess it (Joint Warfighting Center, 2006). By modeling system elements and components as nodes, and the functional or physical relationship between the system elements as links between nodes, insight may be gained into the key nodes (system elements) which are related to multiple systems and which are related to a strategic or operational effect. Modeling an aircraft as a system-of-systems for analysis of key nodes and important functional links may give a valuable perspective on which system elements within the aircraft are most critical to the mission effectiveness and most vulnerable to attack.

Failure Mode Analysis

For modeling the ways that a physical vehicle or system could fail, one of the earliest methodologies used was FMEA, failure mode and effects analysis (MIL-P-1629, 1949). This technique codified a systematic process for analyzing a system with fault tree analysis to determine all the potential ways a system could fail, the causes and effects of the failure, and ways to mitigate the failure. The damage effects were categorized into catastrophic, critical, marginal, and minor failures, and included both direct effects and

secondary effects. The early FMEA process was refined, and utilized in the space program in the 1960's -- essentially the same method used today (NASA, 1966). The name for the process was changed to FMECA, failure mode, effects, and criticality analysis, and is used to systematically analyze all space vehicle systems and subsystems, and require formal acceptance of any residual system risk identified in the process. The overall intent of the FMECA process is a high degree of confidence in the system achieving mission goals.

The FMECA methodology was later expanded to include not just the failure mode causes and effects, but also to analyze the criticality of the failure (MIL-STD-1629A, 1980). The technique was expanded to capture the expected frequency of occurrence of any given failure mode, and the occurrence was factored in to the final analysis of how critical of a risk that failure mode presented, with the idea that if the frequency of occurrence of the failure mode was infinitesimally low, even a failure mode with very severe effects was not highly critical. In this way, the severity and frequency of the failure mode combined to produce a criticality value, which project managers could then use to make program decisions. Figure 2 depicts a commonly used graphical view of how severity and occurrence frequency combine to produce an overall risk level. The process must be iterative to correspond with the design process, and tailored to the requirements of the individual program. A well-executed FMECA is “invaluable to those who are responsible for making program decisions” and uncovers information on the feasibility and adequacy of the system's design (MIL-STD-1629A, 1980).



**Green = Low risk, Yellow = Moderate risk, Red = High risk*

Figure 2: Overall Risk Based on Severity and Occurrence

Later the FMECA process was further refined to include another factor in the overall criticality. Detectability of the failure mode is important, especially in the manufacturing process, as a great deal of time, cost, and effort can be saved if a failure mode cause is detected by quality control, inspection, or some other means (Stamatis, 2003). The failure mode detectability factor is defined as the ability to detect the failure mode before the system reaches the customer. If the failure mode is likely to be detected in the manufacturing process, or through quality control inspections or other means before the system is used, then the detectability rating is low. Conversely, if the failure mode is extremely difficult to detect before the system is used, then the detectability rating is high.

The final metric used in the FMECA process combines the three factors into a single measure. The failure mode's Risk Priority Number (RPN) represents the overall criticality of the failure mode. The RPN is calculated by multiplying the Severity rating, the Occurrence rating, and the Detectability rating together. In this way, all three factors are represented, and not simply in an additive manner. Rather, by multiplying the factors, the interactions between the factors is captured, providing the appropriate rank-ordering of the failure modes by RPN (Stamatis, 2003).

After computation of the RPN, the failure mode is typically categorized as a minor, moderate, high, or critical risk. Corrective actions which must take place are implemented based on the RPN's overall risk category. An example where each factor is at the extreme when rated from one to ten, and causes of risk with the actions taken, is shown in Table 1 (Stamatis, 2003).

Assessment Rating			Causes of failure	Actions taken
O	S	D		
1	1	1	Ideal situation (goal)	No action
1	1	10	Assured mastery	No action
1	10	1	Failure does not reach user	No action
1	10	10	Failure reaches user	Yes
10	1	1	Frequent fails, detectable	Yes
10	1	10	Frequent fails, reaches user	Yes
10	10	1	Frequent fails with major impact	Yes
10	10	10	Trouble!	Yes!!
O=Occurrence, S=Severity, D=Detectability				

Table 1: FMECA Factor Breakdown, Extreme Ratings

Execution of the FMECA process is typically done by a cross-function, multi-disciplined team. The team must understand the system, anticipate its problems and failures, and accurately assess those failures' severity, occurrence, and detectability. An example worksheet used by the analysis team during the FMECA process is shown in the Appendix. This worksheet captures each step of the process and summarizes the results for the program manager. The steps of the overall FMECA process are summarized in Table 2 (Stamatis, 2003).

Eight-Step FMECA Method:
Select team and brainstorm
Functional block diagram and/or process flowchart
Prioritize tasks
Data collection
Analysis
Compilation of Results
Confirm/evaluate/measure results
Iterate/repeat

Table 2: The FMECA Process

FMECA has been applied typically to products during the design and manufacturing process to analyze physical failure modes. However, the use of FMECA has been proposed as applicable for analyzing real-time control systems (Goddard, Validating the Safety of Real-Time Control Systems Using FMEA, 1993) which moves into the realm of failure modes which are not physical in origin. Software reliability has been analyzed by introducing software FMEA techniques (Goddard, Software FMEA Techniques, 2000), however these techniques did not address the overall criticality of the software failure; rather they are only focused on the existence of the failure mode and its effects. The steps involved for accomplishing a successful software FMEA have only recently been codified (Carlson, 2012), as the vast majority of applications which have been published use FMECA to analyze overall criticality of physical failure modes only.

III. Methodology

Overview

This paper proposes to use the basic Failure Mode Effects and Criticality Analysis (FMECA) methodology, as presented in MIL-STD-1629A (1980) and Stamatis (2003), but with modifications to the typical way FMECA is applied for application in information assurance of airborne systems. The method we present here is a proposed way to assist airborne system program managers in prioritizing and focusing their time, money, and personnel efforts on the information assurance risks that present the most significant overall threat to the aircraft and its missions. The FMECA application given is considered a "System" level FMECA (also known as Concept FMECA), applies early in the design process and analyzes the system and subsystems focusing on potential failure modes between the functions of the system, including interactions between different elements of the system (Stamatis, 2003). The System FMECA operates from a conceptual, logical, block-diagram level of detail, and its output includes a potential list of failure modes; a potential list of system functions that could detect potential failure modes; and a potential list of design actions to eliminate failure modes, reduce their occurrence, or mitigate their severity.

The justification for changing the basic FMECA methodology follows. First, the "Occurrence" factor in the FMECA Risk Priority Number (RPN) calculation does not apply to an information assurance failure mode the same as in a physical system failure mode analysis. For a physical system, such as an engine, the Occurrence factor is likely to be scientifically computed through testing or engineering analysis. The reliability and service life of each part of a physical system is likely modeled using a moderately well-

known distribution, such as the number of engine cycles until an engine blade fails, or the likelihood of a defective engine blade, based on the physical properties of the object and known engineering principles. When we speak of the Occurrence of an information assurance failure mode, however, no amount of testing or engineering analysis of an actual physical object can provide a predictable distribution for the likelihood of any specific frequency of occurrence. The failure mode of an information system is not due to material properties and reliability, but rather due to human actions taken to attack a system, or due to human actions which negligently open up vulnerabilities in the system. Thus, a redefinition of how the Occurrence factor applies in the context of information assurance FMECA is necessary.

Secondly, the "Detectability" factor in the FMECA RPN similarly does not apply the same way as in physical system failure modes. In other FMECA methodologies, Detectability refers to the ability to detect the failure before the system reaches the customer (Stamatis, 2003). For example, in an engine a significant failure mode is a crack in the fan blade which causes catastrophic engine failure; the Detectability factor would be high if there were no way to find the defective, cracked fan blade during production before it reaches the customer, but low if quality control inspection or scanning of the engine blades is done in the production process, decreasing the likelihood the defective fan blade reaches the customer. In the case of an information assurance failure mode, however, we assume that a failure mode present in one aircraft is present in all aircraft, and that any failure mode detectable by the manufacturer is prevented or mitigated before reaching the customer. For example, if a data transmission device lacks exception handling capability, and could be easily overwhelmed with invalid messages

that it cannot process, thereby preventing it from functioning, this failure mode would be a problem for every aircraft with the device. The Detectability factor rating loses significance in the context of information assurance failure modes, therefore, as the question becomes not whether the failure mode can be found before reaching the customer, but whether it can be found at all? Since this is impossible to accurately predict, we need a new definition of Detectability if we are to utilize Detectability as a factor in the Risk Priority Number.

The third pillar of the FMECA RPN, "Severity," does not need any unique modifications to the typical FMECA meaning of the term. Severity is the seriousness of the failure mode, as assessed by its impact on the aircraft's safe operation or mission effectiveness. A similar definition of Severity is used in any FMECA method. One important distinction to note, however, is that a failure mode in an aircraft system is likely to put more systems at risk than just the operation of that specific system. Due to the vast complexity of airborne systems, and the dependencies of one system on another, a failure mode in one system may cause degradation and increased risk of failure in another, interrelated system. We further explore this interrelation between systems, and indirect or cascading effect risks, as a follow-on to the FMECA methodology RPN factor definitions which we discuss next.

Information Assurance FMECA Methodology: Occurrence Defined

The Occurrence of an information system threat is inherently unpredictable, as failures depend not on physical stress or wear-and-tear on a component, but rather depend on a wide range of unknowns. These unknowns might include enemy attacker capabilities, insider help, enemy knowledge of the system, system firewalls, safeguards,

access modes, user error, user monitoring, risk mitigation processes, and more. These contributing elements combine to form the overall likelihood of Occurrence of an information system failure mode. As historical data on a failure mode's frequency of Occurrence for a new aircraft system is usually unavailable, subject-matter expert judgment and analysis must be utilized to determine the Occurrence rating for any given failure mode.

To model expert judgment, a scale is needed to quantify the Occurrence rating. The metric used is clearly at the discretion of the project management, in particular how they define what is a negligible rate of Occurrence, what is minor, moderate, high, or severe. One can argue, however, that the overall scale used ought to cover the entire range of all possibilities – the ratings should be collectively exhaustive of all possible Occurrence rates. We present here a possible discrete scale from one to ten; other scales are equally valid based on management preference. A failure mode deemed "impossible" by experts should have an Occurrence rating of one. It might be argued that if it is impossible, the rating should be zero, precluding the need for any further mitigation or risk management; however, we can say that nothing in information systems is truly impossible, as every code has been broken and every impenetrable defense has been breached at some point during the history of warfare (with the possible exception of Navajo code-talkers messages) (Shaw, 1997). Similarly, a failure mode that will occur on nearly every mission should be given an Occurrence rating of ten. For example, if one cannot send a message after their email inbox exceeds a threshold, and that threshold is exceeded on a daily basis, then the Occurrence likelihood of inability to send email is a ten as it is certain to occur regularly.

Between the top and bottom of the scale, from certain Occurrence to impossibility, the definitions of various Occurrence ratings will vary widely. We only state here that the metric used should be clearly defined and unambiguous, removing analyst subjective judgment when executing the information assurance FMECA method, and the ratings should be mutually exclusive in their definitions. The "clairvoyance test" applies – that a clairvoyant who knew precisely what the Occurrence rate of a failure mode will be in the future should have no trouble deciding which Occurrence rating to give to that failure mode.

Here we present a possible scale for evaluating the Occurrence rating for information assurance FMECA:

Example Occurrence Rating Scale	
1	Impossible – should never occur
2	Possible only with insider help / sabotage
3	Possible only with multiple hardware & software failures
4	Possible only with large enemy resources, time, effort, and luck
5	Possible with moderate enemy knowledge / sophistication
6	Possible with little enemy expertise
7	Likely to occur rarely via enemy or unintended means
8	Likely to occur occasionally via enemy or unintended means
9	Will definitely occur on a sporadic basis
10	Will definitely occur on a regular basis

Table 3: Example Occurrence Rating Scale

We note that although historical data on how a particular system may be attacked and the likelihood of it occurring may not be available, data is available on the frequency of attack of other information systems in our society. Unfortunately, many private companies do not share with the public their knowledge of how, where, and when their information systems were attacked, because they perceive little to no benefit from doing so. Some government agencies may have data on the frequency of occurrence of various

types of cyber attack. However, if data becomes available on the Occurrence likelihood of similar attacks on similar systems to those used in the airborne system under analysis, the historical frequency of Occurrence might be utilized to help choose the right Occurrence rating during the FMECA study.

Information Assurance FMECA Methodology: Detectability Defined

The typical definition of Detectability used in FMECA methodologies, the ability to detect a failure before it reaches the customer, does not apply well to the information assurance domain. As noted in the review of articles discussing information system vulnerabilities and failures across other platforms, we noted that the time delay before a failure mode is observed and can be reacted to by the user has a significant, damage-multiplying effect on the severity of the failure, especially in the airborne system environment (Barker, 2011). Likewise, in the information assurance realm, security breaches can exist undetected for extended time periods (weeks, months, or longer). While remaining undetected, exploitation of the system during that time may cause greater and greater damage as time goes on.

Thus, we conclude that a useful definition of Detectability rating is the amount of time between the occurrence of the failure mode and the time the user observes and reacts to mitigate the failure. Note that this time period may vary based on the attentiveness of the aircrew or user, or based on the specifics of system monitoring and built-in checks. Therefore the time period after which the detection of the failure is known has some unknown probabilistic distribution.

The possible distributions for the detection time of the failure are many, and likely are impossible to predict accurately. A simple metric is needed to quantify what the

airborne system program manager really cares about for failure detection – the longest detection time by which the failure will be observed with near certainty or high confidence. A good metric then for Detectability rating is the amount of time after which a failure mode will be observed and reacted to with 95% confidence. This means that over every possible detection time for the failure mode, 95% of these detections will occur at or before the chosen Detectability threshold. This removes the need to specify a specific distribution.

This definition of Detectability removes considering the multitude of possible detection distributions and captures the intent of information assurance failure mode detection. The scale that is produced for specific Detectability ratings based on this definition again falls to the discretion of the program manager. Much like Occurrence rating, the Detectability rating scale should be collectively exhaustive and mutually exclusive among all ratings. A proposed example scale is presented here for evaluating the Detectability rating for information assurance FMECA:

Example Detectability Rating Scale	
1	Certain, immediate detection by all crew/users/systems
2	Certain, immediate detection by one crew/user/system
3	Probable detection by all crew/users/systems
4	Probable detection by one crew/user/system
5	Improbable immediate detection, probable detection within minutes
6	Probable detection within hours
7	Probable detection before the next mission
8	Possible detection within a few missions
9	Possible to detect only after many missions
10	Impossible to detect over many missions
	*Time periods listed are considered a 95% confidence of detection at or before the given time

Table 4: Example Detectability Rating Scale

A trait of the information assurance domain is that a breach of system security may result in not only an immediate threat to system availability, integrity, or confidentiality, but may be an opportunity for an attacker to embed malicious code that allows later follow-on attacks with more ease, or that enables attacks on other related systems. A breach in one system or component may be detectable quickly, but may produce other breaches which are less detectable. This complicates the Detectability rating significantly, and must be accounted for in the analysis of the Detectability failure mode. Detectability may also depend upon security and monitoring procedures which may not be implemented or determined at the time of the FMECA analysis, which further complicates its assessment. Underlying the Detectability rating is the high likelihood that the enemy may be doing everything they can to mask the detection of a security breach or exploitation, making Detectability problematic to assess and a significant concern that system designers should address as early as possible. Modifications to a system after fielding to improve failure mode detection may be costly and difficult to implement. Inclusion of monitoring and warning flags in the original system design, while cumbersome, may be far less costly and difficult in the long run.

Information Assurance FMECA Methodology: Severity Defined

We close our presentation of information assurance FMECA methodology with a definition of the Severity factor rating. Severity is the seriousness of the failure mode, as assessed by its impact on the aircraft's safe operation or mission effectiveness. The Severity of a failure mode should be assessed by a team of experts who can analyze not only the information systems involved, but also the use and mission-related functions of the system. For airborne systems, expert aircrew members who actually use the systems

in question must weigh in on the possible effects of the failure mode to produce a sound Severity rating. Other personnel whose knowledge may be valuable in assessing Severity are maintenance experts, communications experts, even ground personnel experts who control, utilize, or otherwise interact with the aircraft's systems and may depend on their reliable functionality.

We present here one possible scale of mutually exclusive, collectively exhaustive Severity ratings which may be utilized for failure modes in the information assurance FMECA methodology:

Example Severity Rating Scale	
1	No distraction & no mission / flight safety impact whatsoever
2	Nuisance only, distraction with no mission impact
3	Loss of system inconvenient but no mission / safety impact
4	Low impact on mission effectiveness
5	Moderate mission effectiveness impact
6	Severe mission effectiveness loss, no safety of flight impact
7	Minor safety of flight impact
8	Severe safety of flight impact
9	Catastrophic destruction of the aircraft
10	Catastrophic destruction of multiple aircraft/missions

Table 5: Example Severity Rating Scale

The Severity of a failure mode in an aircraft system is likely to put more systems at risk than just the specific system with the vulnerability. An airborne system is a highly complex system of systems, and the interrelated nature of their functioning causes the failure to potentially have many indirect or cascading effects. Since the combinations of possible indirect effects are numerous, should these indirect effects be considered in assessing the Severity rating of a failure mode? From a system-of-systems analysis

perspective, effects in complex systems can certainly ripple throughout other systems (Joint Warfighting Center, 2006).

We argue that indirect effects should not factor in to the Severity of the failure mode. The failure mode Severity should accurately reflect the seriousness of the specific failure in question. To account for the cascading or indirect effects of a failure on the remainder of the airborne system, we propose that the indirect effects generated from a failure mode of one system generate new, additional failure modes of the related systems. In this way, the analysis is appropriately expanded to include all possible repercussions of the failure mode. Essentially, a new failure mode is produced for each possible indirect effect of a direct failure mode.

For example, consider a failure mode of the aircraft's air data system which helps produce erroneous altitude information. This in itself may cause some mission impact and so the Severity level depends on the system redundancies and the amount of degradation produced. If the altitude data from that system, however, is utilized by the engine management system, then an indirect effect of the altimeter degradation might be that the aircraft's engines are operated outside their design operating parameters, causing possible engine overheating, flameout, or failure. The Severity of the original air data system failure mode should not include the possible seriousness of the indirect effects on the engine management system; rather, a new failure mode is generated based on erroneous altitude inputs into the engine system. Perhaps the engine system does not have in itself any vulnerabilities which might be attacked from an information system threat perspective – but through indirect effects of the vulnerabilities of another system, it can be affected, and such additional, indirect failure modes must be considered.

Putting It All Together: Information Assurance FMECA Execution

Once the scales for Occurrence rating, Detectability rating, and Severity rating are defined, information assurance FMECA can begin analyzing specific failure modes. The overall process consists of a sequence of steps to characterize the failure mode, rate it, detail possible indirect or cascading effects, and suggest mitigation methods to reduce overall system risk. These steps are iterated over all aircraft systems and all information system threats.

Information Assurance FMECA Process	
1	Select rating scale definitions
2	Select team and brainstorm failure modes
3	Collect data on failure modes
4	Analyze failure mode ratings
5	Develop indirect / cascading effects failure modes
6	Evaluate results and prioritized rankings
7	Brainstorm mitigation methods in priority order
8	Implement mitigation
9	Repeat analysis with new data / measures
10	Iterate process over all systems / vulnerabilities

Table 6: Information Assurance FMECA Process

Brainstorming failure modes and collecting data on them may prove very problematic in the information assurance realm. As seen in the history of cyber attacks, some attack methods may be entirely unanticipated by the analysis team. Certainly, new cyberspace threats may arise at any time, just as new ways of jamming or deceiving radar systems arose throughout the late twentieth century.

Generally, vulnerabilities in the security of communications or computer systems can be broadly classified into one of three classes. These classes are defined as attacks that:

1. Block (deny) communications of legitimate use
2. Intercept communications, allowing enemy exploitation
3. Fabricate communications which are not legitimate
4. Are combinations of 1 – 3 above.

Based on one of these methods, the communications nodes or links in the system are attacked. The specific method of the attack may vary widely. One should consider broadly all the types of attacks listed below in Table 7, and any other type of attack possible based on specific characteristics of the information system.

Common Information Assurance System Threats / Vulnerabilities
- Distributed Denial of Service Attack
- Signal Noise Jamming
- Signal Deception / Repeater Jamming
- Access through coding flaws
- Protocol weaknesses
- Unintentional data/signal paths
- Intentional data/signal paths not protected
- Exploitation of system trust relationships
- Exploitation of code vulnerabilities
- Fuzzed inputs
- Exploitation of system updates/maintenance
- Unintentional user error or maintenance error
- Insider access from solo source
- Insider access from multiple sources
- Sabotage

Table 7: Common Threats / Vulnerabilities

Effects are developed after determining the range of possible types of attacks a system may face. Generally, an attack on an information system compromises one or more of the three main pillars of information assurance: Confidentiality, Availability, or Integrity. For an airborne system, compromise of the integrity or availability are likely to cause problems with safety of flight, particularly if the system is used to control, navigate, or protect the aircraft. Confidentiality of airborne systems is less likely to

present an immediate threat to safety of flight, but may threaten safety over time (for example by informing the enemy of the aircraft's exact position and altitude, so that it may be targeted by kinetic weapons). In any case, expert aircrew (preferably certified for developmental test and evaluation) should be consulted as part of the analysis process for determining vulnerability consequences.

For airborne systems not directly supporting the aircraft's safety of flight, but rather supporting another mission role, an information system attack could compromise any or all of the IA pillars, confidentiality, availability, or integrity. Some airborne systems may have crucial information which must be kept confidential from the enemy, such as aircraft flight plan routings or radar data. Some systems, like threat warning systems, may be needed at a moment's notice in flight, so the availability is critical. For most systems, the integrity of the resident information is mission essential. Depending on the nature of the system and the information it processes, any of these could cause severe loss of mission effectiveness – expert operators of the system must be consulted as to the effects.

Determination of the likelihood of Occurrence of these types of threats, and the Detectability of each, will vary from system to system. Multidisciplinary cooperation among information system, electronic system, maintenance, aircrew, and engineering teams is needed to accurately evaluate the failure modes resulting from listed threats/vulnerabilities. The corresponding FMECA ratings must account for what is known about the brainstormed vulnerability and failure mode, and should include what is possible but unknown about these threats.

In addition to brainstorming threats and vulnerabilities, the analysis team should brainstorm potential ways to mitigate the risks found during the FMECA process. Consideration should be given to the types of controls that might be used to decrease the Occurrence, Detectability, or Severity ratings. Some risks might only be mitigated through physical hardware changes, through building in or adding redundancies, or through actual software protocols that prevent or at least monitor for the failure mode in question. Other risks, however, might be mitigated by procedural processes, which may be quicker and less costly than the hardware or software solutions. The multidisciplinary team of experts doing the analysis should consider any and all means available to reduce the overall risk of each failure mode. Ideally the Severity of every risk would be minimized so that no threat is more than a nuisance – certainly this will not be possible in every case, however, so mitigation by improving the Occurrence or even just the Detectability of a failure mode might be sufficient to give program managers confidence in the airborne system's overall safety and effectiveness.

Note, that the methodology proposed here is not intended to be the only FMECA method used in assessing risk to the airborne system. As noted by several authors, for the most benefit, the FMECA should be initiated as soon as preliminary design information is available, and progressively developed along with the system design, through production, and even throughout the product's entire life-cycle (Stamatis, 2003; MIL-STD-1629A, 1980). Only through such diligence can risks be accurately assessed and mitigated (or knowingly accepted) as the product, its vulnerabilities, and the external threats change throughout the product's life.

Presenting the Results and Using the Results for Decisions

Once the analysis team has detailed the information assurance failure modes, and calculated the associated FMECA RPN for each, the information is summarized and reported. An example FMECA worksheet for displaying the FMECA failure mode, Occurrence, Detectability, Severity, RPN, indirect effects, mitigation, and more is shown in the Appendix. Worksheets similar to the one presented can be used for summarizing FMECA results in easy-to-read format for managers' reference.

The primary products of the FMECA process are the RPN and the possible mitigation methods. Mitigation methods will vary widely. RPN, however, is a simple scalar number that will not inherently mean anything to a manager. The key to understanding the significance of the RPN is to know what values of RPN a manager should fear, should be concerned, or should be comforted in seeing. The exact RPN, as a product of the Occurrence, Detectability, and Severity factors, will depend on the scales used for each factor. If a one-to-ten scale is used for each factor as suggested in the example scales above, then the final RPN value will be between 1 and 1000 for each failure mode. This final RPN provides a relative priority between failure modes, for the manager's use for prioritizing time, money, personnel and other resources into fixing or mitigating. The overall risk criticality represented by the RPN must be classified into levels of overall risk. The “red/yellow/green” for low/moderate/high risk method of Figure 2 is one way to think about classification of overall risk criticality.

A net or spider diagram may be useful to visualize the different RPN values resulting from each failure mode. For example, suppose three failure modes were found, with factors as listed in Table 8.

Failure mode	Occurrence	Detectability	Severity	RPN
1	2	5	9	90
2	5	4	6	120
3	8	1	3	24

Table 8: Example Failure Mode RPN Values

In this example, failure mode 2 has the highest RPN and is therefore the highest priority for the managers to mitigate; failure mode 1 is next and failure mode 3 is lowest priority. One can visualize the factors that contribute to the RPN using a spider diagram as shown in Figure 3, with an axis for each factor, and the distance along that axis which is shaded representing the magnitude of that factor.

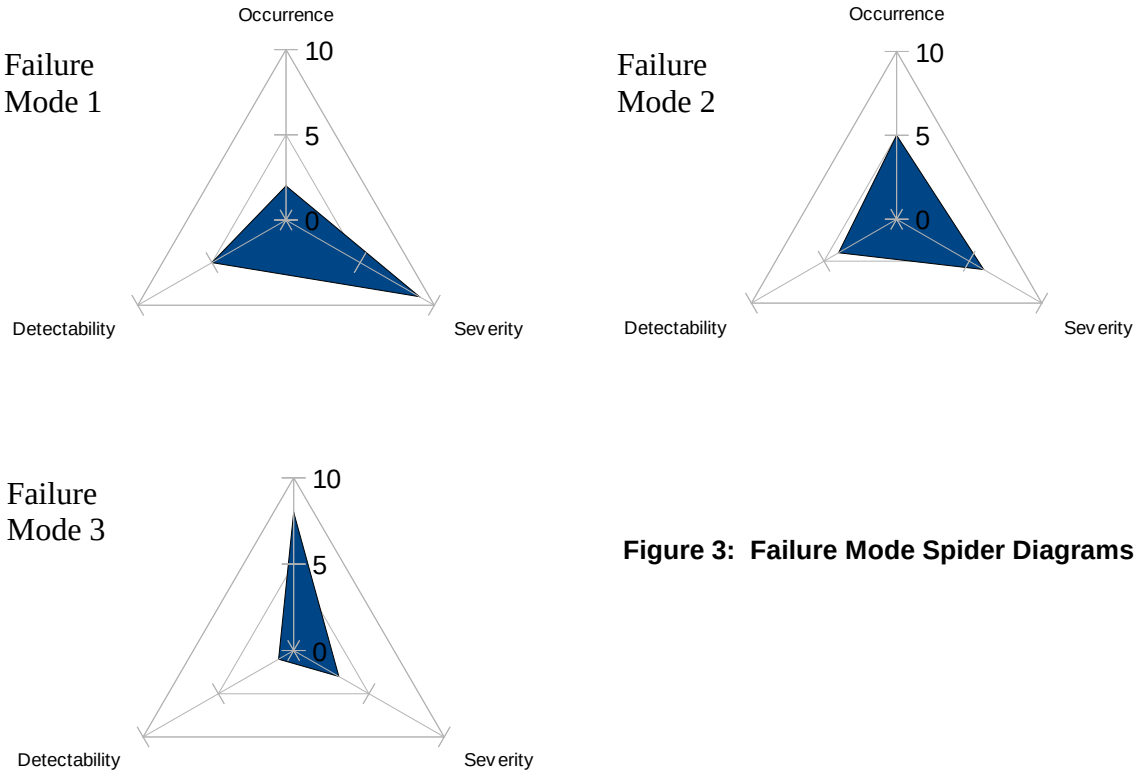


Figure 3: Failure Mode Spider Diagrams

The shaded area along each axis corresponds to the magnitude of the RPN factor for that axis. Note that the apparent area of the resulting shaded regions for failure modes

1 and 2 are of similar size, yet failure mode 2 has the higher RPN. This is due to the three-dimensional nature of the RPN which makes it more difficult to visualize. Failure modes 1 and 2 do have RPN values of roughly the same magnitude (RPN 90 and RPN 120). The spider diagram provides a quick look at how critical the risk of the failure mode is, but the exact values are needed to rank-order failure modes by risk priority.

Specific actions by project managers for various RPN levels are at their discretion. One could suggest having a clear policy on the manager's intent for various ranges of RPN values. An example policy might be to categorize RPN values into classifications of risk level, and mandate further analysis or mitigation of the failure mode depending on the RPN classifications. A sample policy is presented in Table 9. This RPN policy scheme assumes a total RPN scale of 1 to 1000, using RPN factors on a scale of 1 to 10 each.

Risk Priority Number Policy

Final RPN Range	Actions Required
1 to 15	No action necessary – program manager accepts risk
16 to 50	Minor effort – design team implement mitigation as available and only at low cost – no major redesign of system
51 to 120	Major effort – significant mitigation required – major redesign not preferred – high cost changes justified
121 to 1000	Program at severe risk – complete/major redesign justified at any cost – mitigation required before development proceeds

Table 9: Example RPN Manager's Policy

Note that the example policy standard presented is highly dependent on the specific scales used for each RPN factor. Other possible policies on RPN or its factors

are certainly possible. The manager may want to have a policy on failure modes with very high values in a single factor, for instance. A policy might be that any failure mode with a Severity factor greater than 7 (severe safety of flight impact) must be mitigated down to Occurrence and Detectability each below 3 (possible only with insider help, and immediate detection by an operator). Another policy might be that any failure mode with a Detectability factor greater than 8 must have design changes put in place so that it becomes detectable in a quicker time. The management's options on RPN policy are many, but a good understanding of the definitions of each factor is important, and sound judgment on the impact of the various risk combinations is needed for maximum information assurance security effectiveness at minimum cost.

IV. Case Study Results and Analysis

Overview

We now examine several notional, yet possible, information assurance failure modes for an airborne system. We provide five descriptions of failure modes, and break down how each is analyzed using the information assurance FMECA method and scales presented in the prior section. We conclude with a comparison of the five failures and show a sample worksheet suitable for management review. Note: The failure modes presented are hypothetical only, they do not represent an actual aircraft's systems operations nor necessarily any actual vulnerabilities to any of the systems discussed. The results shown are complete, meaning we include mitigation strategies which would normally require in-depth work by the engineering and analysis team.

Case 1: Denial of Service Attack on Transponder System.

Description of Failure Mode: The aircraft's Identification Friend-or-Foe (IFF) Mode S transponder is bombarded with false signals. These false signals appear to the transponder's communications processor as legitimate queries of aircraft position, and require the aircraft transponder to transmit its current position and altitude in reply to the signal. The constant bombarding of the transponder with this query results in the inability of the transponder to complete its normal functionality. As a result, legitimate air traffic controller systems are unable to communicate with the aircraft's transponder. Voice communication using the aircraft's radios is needed to provide air traffic control properly.

Aircraft System: IFF Mode S transponder, model XYZ-123.

Potential Failure Mode: Denial of Service Attack – false signal bombardment.

Potential Effects: Transponder inoperative / unusable for legitimate purposes.

Detection Method: Aircrew may detect lack of air traffic control transponder messages after several minutes. Air traffic controllers may detect lack of aircraft response to legitimate ATC messages after several minutes.

Ratings: Occurrence = 6: possible with little enemy expertise.

Detectability = 5: improbable immediate detection, probable detection within minutes.

Severity = 3: Loss of system inconvenient but no mission / safety impact.

Risk Priority Number (RPN) = 6 x 5 x 3 = 90.

Possible Indirect or Cascading Effects:

1. Constant load on transponder processor causes aircraft communications bus to degrade. Slow response from other systems on communications bus.
2. Constant emission of transponder signals degrades radio frequency environment / electromagnetic spectrum near aircraft threat warning antennas. Slowed / degraded response of threat warning system to certain wavelength threats.

Recommended Actions:

1. Modifications to the IFF processor software to prevent inoperative transponder. Use of signal filtering / prioritization logic to discard repeated low priority signals.
2. Additional aircraft caution message generation and display, to alert

aircrew immediately of saturation of transponder processor.

Responsible Office: Aircraft communications system engineer, transponder specialist.

Actions Taken: None. Planned upgrade to IFF transponder 5/2013.

Date Implemented: TBD. Planned upgrade to IFF transponder 5/2013.

Mitigated Ratings: Occurrence = 3: possible only with multiple hardware / software failures.

Detectability = 3: probable detection by all crew/systems/users.

Severity = 3: unchanged.

Mitigated RPN: 3 x 3 x 3 = 27.

Case 2: Exploitation Attack on Threat Warning System.

Description of Failure Mode: The aircraft's internal communications bus is compromised by unauthorized access at the maintenance level, via stolen or hacked password/authentication. Electronic logic filters are adjusted within the internal bus to block certain messages from the threat warning system antennas from reaching the threat warning system central processor. This causes certain enemy radar systems threats to be blanked from aircrew displays when they are targeting the aircraft.

Aircraft System: Communications bus, LMNOP-456.

Potential Failure Mode: Unauthorized message filter preventing threat display/warning.

Potential Effects: Aircrew unaware of being targeted by enemy radar systems; countermeasures and counter-tactics not used. Potential catastrophic loss of mission/crew via secondary threat.

Detection Method: Aircrew are unlikely to detect the threat blanking in-flight. Possible detection of unauthorized message filter logic by maintenance during periodic checks/system scans after one or more missions.

Ratings: Occurrence = 4: possible only with large enemy resources, time, effort, and luck.

Detectability = 8: possible detection within a few missions.

Severity = 9: catastrophic destruction of the aircraft.

Risk Priority Number (RPN) = 4 x 8 x 9 = 288.

Possible Indirect or Cascading Effects: None.

Recommended Actions:

1. Change of access permissions/procedures to require multiple screenings and multiple reviews for all maintenance updates to communications bus software.
2. Integration of short-lifespan cryptographic keys as necessary to update bus software.
3. Periodic, automatic communications bus built-in-test added to monitor signal passage and receipt with threat warning system antennas. Generation of warning/caution on crew displays for improper operation.

Responsible Office: Aircraft communications system engineer, threat warning system specialist; bus software specialist; maintenance specialist; cryptographic specialist.

Actions Taken: None. Planned upgrade to communications bus 7/2012.

Date Implemented: TBD. Planned upgrade to IFF transponder 7/2012.

Mitigated Ratings: Occurrence = 2: possible only with insider help / sabotage.

Detectability = 1: certain, immediate detection by all crew/systems/users.

Severity = 9: unchanged.

Mitigated RPN: 2 x 1 x 9 = 18.

Case 3: Dormant Malware Attack on Instrument Landing System / Navigation System.

Description of Failure Mode: The aircraft's Instrument Landing System (ILS) and Navigation System are attacked with malware via network means through the communications bus. Dormant malware is placed in the ILS and Navigation systems which activates when the aircraft is on active ILS approach to a runway and low to the ground. The malware causes erroneous ILS indications and coordinated Navigation indications which make the aircraft appear to be on course for the runway, but actually be flying into the ground away from the airport. Erroneous navigation data is also passed to the transponder system which decreases the likelihood that air traffic controllers will notice the aircraft's true position. Aircraft flight safety at risk, especially for landing at night or in bad weather.

Aircraft System: ILS system, FGH-789, and Navigation system, IJK-210.

Potential Failure Mode: Network Attack – dormant malware installed.

Potential Effects: Night or bad weather landing navigation extremely difficult; potential loss of aircraft.

Detection Method: Aircrew may detect the erroneous navigation information but based on the dual ILS and Nav coordination, this is unlikely. Air traffic controllers may detect raw radar returns off course, but since transponder is fooled, they might not see the true aircraft position.

Ratings: Occurrence = 4: possible only with large enemy resources, time, effort, and luck.

Detectability = 7: probable detection before the next mission.

Severity = 9: Catastrophic destruction of the aircraft.

Risk Priority Number (RPN) = 4 x 7 x 9 = 252.

Possible Indirect or Cascading Effects: Erroneous transponder signals sent based on erroneous navigation info.

Recommended Actions: Modifications to the Navigation system to prevent malware infection through network means.

Responsible Office: Aircraft network engineer, navigation system engineer.

Actions Taken: None. Planned upgrade to Navigation system 8/2012.

Date Implemented: TBD. Planned upgrade to Navigation system 8/2012.

Mitigated Ratings: Occurrence = 1: impossible – should never occur.

Detectability = 7: unchanged.

Severity = 9: unchanged.

Mitigated RPN: 1 x 7 x 9 = 63.

Case 4: Malicious Software Update Attack on Fuel Management System

Description of Failure Mode: The Fuel Management System software is attacked by insertion of enemy-developed software files, which are placed on the Fuel Management System commercial vendor's site and appear as valid updates to Fuel Management System software. Software, once installed by maintenance using normal update procedures, then causes inflight opening of fuel ports, dumping fuel from the aircraft, locking out some fuel cells, and contaminating other fuel cells with water vapor. Additionally, fuel contamination can spread to other aircraft via inflight refueling conduits.

Aircraft System: Fuel management system, PQR-654.

Potential Failure Mode: Invalid software update attack.

Potential Effects: Loss of fuel; contamination of fuel cells; lockout of fuel cells; passage of contaminated fuel to other aircraft. Catastrophic loss of multiple aircraft.

Detection Method: Initial indications of fuel dumping / vents open masked from crew display by software. Aircrew may detect fuel dumping after minutes or hours depending on the rate. Aircrew will detect engine problems when contaminated fuel reaches the engines.

Ratings: Occurrence = 4: possible with large enemy resources, effort, time, and luck.

Detectability = 6: probable detection within hours.

Severity = 10: catastrophic destruction of multiple aircraft/missions.

Risk Priority Number (RPN) = 4 x 6 x 10 = 240.

Possible Indirect or Cascading Effects:

1. Engine failure due to fuel contaminated with water vapor.
2. Engine failure for other aircraft who receive contaminated fuel via inflight refueling.
3. Engine flameout due to lack of fuel caused by fuel cell lockouts and fuel dumping.

Recommended Actions:

1. Change of access permissions/procedures to require multiple screenings and multiple reviews for all maintenance updates to fuel management software.
2. Integration of short-lifespan cryptographic keys as necessary to update fuel management software.
3. Backup fuel system installation to allow manual monitoring and manual control of fuel vents / valves / transfer components.

Responsible Office: Aircraft fuel system engineers, maintenance specialists.

Actions Taken: Redesign fuel management system for backup operation 6/2012.

Date Implemented: TBD. Redesigned system implemented immediately for production and retrofit for fielded aircraft.

Mitigated Ratings: Occurrence = 2: possible only with insider help / sabotage.

Detectability = 4: probable detection by one crew/systems/users.

Severity = 7: minor safety of flight impact once backup fuel system activated.

Mitigated RPN: 2 x 4 x 7 = 56.

Case 5: Signal Blockage to Braking System

Description of Failure Mode: The aircraft braking system, via aircraft bus buffer overload, is denied the signal which tells it whether the aircraft's landing gear is extended or retracted. Its default operation is to assume landing gear is retracted, in which case it locks all brakes to prevent wheel motion inside the gear wells. When failure mode occurs, wheel brakes remain locked after gear is extended, causing blowout of all tires upon impact with the runway.

Aircraft System: Aircraft data bus, TUV-987; wheel brake sensors, WXY-345.

Potential Failure Mode: Buffer Overload Attack – block of landing gear position signal.

Potential Effects: Wheels locked during landing – tire blowout for all tires – loss of aircraft directional control on the runway – possible loss of aircraft.

Detection Method: Aircrew are unable to detect brake status in the cockpit. Detection likely to occur only as aircraft lands.

Ratings: Occurrence = 5: possible with moderate enemy knowledge / sophistication.

Detectability = 7: probable detection before the next mission.

Severity = 9: catastrophic destruction of the aircraft.

Risk Priority Number (RPN) = 5 x 7 x 9 = 315.

Possible Indirect or Cascading Effects: Tire blowout due to brake lockup. Loss of nosewheel steering due to loss of tires. Hydraulic leaks due to collateral damage from tire blowout.

Recommended Actions: Modifications to braking system to change default logic to assume landing gear is down.

Responsible Office: Aircraft braking system engineer.

Actions Taken: None. Planned modification to braking system 5/2013.

Date Implemented: TBD. Planned upgrade to braking system 5/2013.

Mitigated Ratings: Occurrence = 5: possible only with multiple hardware / software failures.

Detectability = 7: probable detection by all crew/systems/users.

Severity = 1: no distraction and no mission / flight safety impact whatsoever.

Mitigated RPN: 5 x 7 x 1 = 35.

Case Study Summary

We have shown five case study examples of possible information assurance failure modes and the resulting effects on the aircraft systems, flight safety, and mission effectiveness. These examples demonstrated a variety of access vectors to aircraft information systems, including radio frequency signals, network means, unauthorized access, and software vendor maintenance exploitation. The braking system failure mode is a good example of one that may have been generated as an indirect effect of a different failure mode – the data bus buffer overload may have been noted as a failure mode of the bus, and the braking system may have been one of the cascading effects noted since the signal to the brakes was one of the signals impacted in the prior failure mode.

We have also indicated how occurrence and severity of the failure modes may vary among different systems. We identified possible indirect effects, and offered potential recommended actions which mitigate the occurrence, detection, and/or severity risks for each failure mode.

The program manager, once the analysis is finished, can then rank and compare failure modes for management's use in allocation of resources towards mitigation and fixing. A summary of the five failure modes presented is shown in the sample worksheet in Figure 4.

Figure 4: Summary Worksheet Example

Information Assurance FMECA Worksheet			Program: Case Study aircraft Prepared by: C. Middleton		Responsibility:	Case Study manager		Initial analysis date: 5/15/2012 Last update: 6/4/2012						Mitigated Ratings			
Aircraft System	**Potential Failure Mode**	**Potential Effects**	**Potential Causes of Failure**	**Detection Method**	**Ratings Occurrence**	**Detectability**	**Severity**	**Risk Priority Number (RPN)**	**Indirect or Cascading Effects**	**Recommended Action**	**Responsible office**	**Actions Taken**	**Date Implemented**	**Occurrence**	**Detectability**	**Severity**	**Mitigated RPN**
Mode S transponder	Denial of service	Transponder inoperative	False signal bombardment	Aircrew - minutes Air traffic controllers - minutes	6	5	3	**90**	1-Degraded comm bus 2-Degraded threat warning	1-Mod IFF software 2-Add caution message	Comm sys engineer, transponder engineer	Planned 5/13	Planned 5/13	3	3	3	**27**
Threat warning system	Blocked / blanked threats	Lack of threat warning Aircraft shot down	Unauthorized access to comm bus	Maintenance post-flight periodic checks	4	8	9	**288**	None	1-Access changes 2-Crypto keys for updating 3-BIT for antenna comm	Comm engineer Threat sys engineer	Planned 7/12	Planned 7/12	2	1	9	**18**
ILS/Nav system	Erroneous position	Crash during landing	Malware placed through network	Crew/ATC unlikely	4	7	9	**252**	Transponder signal erroneous	Mod nav sys to prevent malware	Network engineer Nav sys engineer	Planned 8/12	Planned 8/12	1	7	6	**63**
Fuel management system	Fuel dumping, fuel cell lockout, fuel contamination	Loss of multiple aircraft	Enemy exploitation of vendor software files, updated onto aircraft	Aircrew - minutes to hours	4	6	10	**240**	1-Engine failure 2-Other aircraft engine fails 3-Engine flameout	1-Change permissions 2-Crypto keys for updating 3-Backup fuel mgmt system redesign	Fuel sys engineer Maintenance specialist	Planned 6/12	Planned 6/12	2	4	7	**56**
Braking system	Blocking of gear extension signal	Tire blowout on landing, loss of aircraft	Data bus buffer overload	Unlikely before catastrophe	5	7	9	**315**	Tire blowout Steering fail Hydraulic leak	Mod braking default logic	Braking sys engineer	Planned 5/13	Planned 5/13	5	7	1	**35**

From the worksheet, the manager can easily see that the most critical current vulnerability is the braking system failure mode, with a RPN of 315. The IFF transponder failure mode has the lowest RPN of 90, with the other three falling between these extremes. The manager can make resource allocation and policy decisions based on these RPN values. Also the manager receives an indication of how the problem can be mitigated and the resulting risk level after the mitigation is implemented, using the Mitigated RPN value. Indirect effects are also listed which will, in turn, generate new failure modes.

Once the analysis team implements the information assurance FMECA process, and applies it across all possible threat access vectors and all possible aircraft systems, the program manager should have a complete picture of the threats and failure modes which are most important to mitigate and which he can be comfortable accepting the risk for without further mitigation.

V. Conclusion

The information assurance FMECA methodology presented provides a systematic way to assess information assurance risks to airborne systems. Many aircraft system failure modes may occur due to information system threats, and due to the increasingly interrelated connections between electronic airborne systems, these failure modes may have significant effects on the aircraft's mission effectiveness or safety of flight.

In gauging the overall risk to the mission and safety, the severity of the failure mode must be determined by expert judgment. In addition, the overall criticality of the risk the failure mode presents depends greatly on the frequency of occurrence of the failure mode and the detectability of the failure mode. These three factors combine in an interactive way to impact the overall risk.

Scales to measure the failure mode's Occurrence, Detectability, and Severity must be clearly defined, with discrete ratings that cover all possibilities in a collectively exhaustive manner, while allowing straightforward, mutually exclusive individual rating definitions. These scales should be based on the aircraft program manager's or certification authority's vision and priorities for their acceptable levels of risk and risk tolerance.

Once the scales are defined and the analysis is executed, the decision maker can apply decision standards to the final Risk Priority Number produced by the analysis. These standards should define the overall risk categories and the mitigation required depending on the risk level. Mitigation methods are integrated into the analysis so that ways to decrease the Occurrence, Detectability, or Severity ratings are generated by the system experts who analyzed the failure mode.

The information assurance FMECA process is an iterative process that applies to all electronic aircraft systems, and must be updated over time as the aircraft design changes. New threats may produce new risks, or newly discovered vulnerabilities may open new means of attack; repetition or revalidation of the information assurance FMECA process is required for a complete, robust perspective on airborne system risk.

Recommendations from this research include the following. Air Force Materiel Command (AFMC) and other Department of Defense organizations should consider applying this information assurance FMECA methodology to their developmental efforts in aircraft acquisition, test and evaluation. Civil aircraft manufacturers and authorities should consider the methodology for broader application in the civil aviation industry as well.

Future research on the topic of analysis of information assurance for airborne systems should investigate the measure theory aspects of the scales used as metrics for scoring the risk component factors to match managerial preferences. The metrics proposed here are notional, and should be validated for specific use, as well as for general use across the spectrum of threats and vulnerabilities. The process for assessing threats and vulnerabilities must be studied, so that information assurance assessment procedures can be standardized. This research focused on quantitative aspects of the information assurance assessment, and processes for executing the assessment itself should be refined. Finally, a fully enumerated listing of information assurance attack types or methods, which estimates the frequency of occurrence of each as well as the detectability of each, is vital research which will clarify greatly our assessments of the information assurance risks to our airborne systems.

Bibliography

Alexander, K. B. (2007). Warfighting in Cyberspace. *Joint Forces Quarterly* .

Barker. (2011). Is Innovative Aerospace Technology Getting Too Far Ahead of Itself? *XCockpit* .

Bilton, N., & Stelter, B. (2011, April 26). Sony Says PlayStation Hacker Got Personal Data. *New York Times* .

Carlson, C. (2012). *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis.* Hoboken: John Wiley & Sons.

Daily Wireless. (2007, May 8). *SkyNet Satellite Hacked*.

Federal Aviation Administration. (2008). *Special Conditions: Boeing 787-8 Airplane; Systems and Data Networks Security--Isolation or Protection From Unauthorized Passenger Domain Systems Access.* Department of Transportation.

Fildes, J. (2011, February 15). *Stuxnet virus targets and spread revealed*. Retrieved from British Broadcasting Corporation.

Fulghum, D., Sweetman, B., & Butler, A. (2012, February 6). China's Role In JSF's Spiraling Costs. *Aviation Week* .

Goddard, P. L. (2000). Software FMEA Techniques. *Proceedings of the Annual Reliability and Maintainability Symposium.*

Goddard, P. L. (1993). Validating the Safety of Real-Time Control Systems Using FMEA. *Proceedings of the Annual Reliability and Maintainability Symposium* .

Gorman, S. (2009, May 7). FAA's Air-Traffic Networks Breached by Hackers. *Wall Street Journal* .

Gorman, S., Dreazen, Y. J., & Cole, A. (2009, December 17). $26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected. *Wall Street Journal* .

Joint Warfighting Center. (2006). *Information Operations.* United States Joint Forces Command.

Joint Warfighting Center. (2006). The System Perspective. *Commander's Handbook for an Effects-Based Approach to Joint Operations* .

Lambeth, B. S. (2011). Airpower, Spacepower, and Cyberpower. *Joint Forces Quarterly* .

Mackenzie, C. (2011, December 15). 'We hacked a U.S. Drone'. *The Christian Science Monitor* .

Marquand, R., & Arnoldy, B. (2007, September 16). China's hacking skills in spotlight. *The Christian Science Monitor* .

MIL-P-1629. (1949). *Procedures for performing a failure mode effect and criticality analysis.* Department of Defense.

MIL-STD-1629A. (1980). *Procedures for Performing a Failure Mode, Effects and Criticality Analysis.* Department of Defense.

Morgan, D. (2011, August 29). *Hackers Attack Air Traffic Control*. Retrieved from ABC News.

NASA. (1966). Procedure for Failure Mode, Effects and Criticality Analysis. *National Aeronautics and Space Administration* .

Poulsen, K. (2003, August 19). *Slammer worm crashed Ohio nuke plant network.* Retrieved from Security Focus.

Shachtman, N. (2011, October 7). *Computer Virus Hits U.S. Drone Fleet*. Retrieved from Wired.

Shaw, J. M. (1997). Intelligence: Code Breaking, Espionage, Deception, and Special Operations. In *World War 2 in Europe, Africa, and the Americas with General Sources.* Greenward Press.

Silver-Greenberg, J., & Schwartz, N. D. (2012, March 30). MasterCard and Visa Investigate Data Breach. *New York Times* .

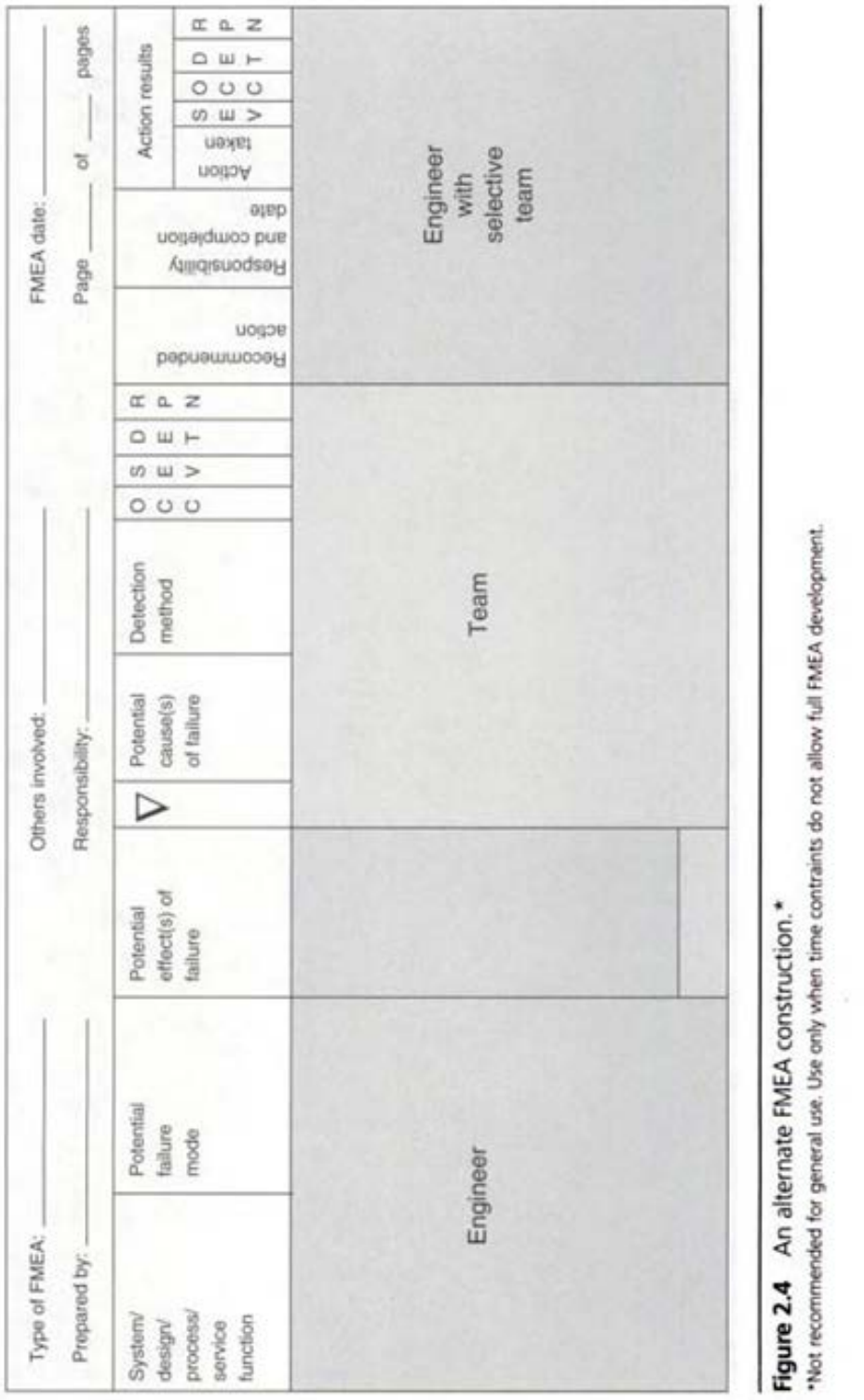
Stamatis, D. (2003). *Failure Mode Effect Analysis: FMEA from Theory to Execution.* Milwaukee: Quality Press.

US General Accounting Office. (2004). *GAO Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform.* House Committee on Government Reform.

Warden, J. A. (1995). The Enemy As A System. *Airpower Journal* .

Appendix

Figure 5: Sample FMECA Worksheet (Stamatis, 2003)



Type of FMEA: _____ Others involved: _____ FMEA date: _____

Prepared by: _____ Responsibility: _____ Page _____ of _____ pages

System/ design/ process/ service function	Potential failure mode	Potential effect(s) of failure	▽	Potential cause(s) of failure	Detection method	O C V	S E T	D E P	R P N	Recommended action	Responsibility and completion date	Action taken	Action results: S E V	O C T	D E P	R P N
Engineer				Team						Engineer with selective team						

Figure 2.4 An alternate FMEA construction.*

*Not recommended for general use. Use only when time contraints do not allow full FMEA development.

Figure 6: Information Assurance

FMECA Worksheet

Information Assurance FMECA Worksheet

Program:
Prepared by:

Responsibility:

Initial analysis date:
Last update:

Aircraft System	Potential Failure Mode	Potential Effects	Potential Causes of Failure	Detection Method	Ratings			Risk Priority Number (RPN)	Indirect or Cascading Effects	Recommended Action	Responsible office	Actions Taken	Date Implemented
					Occurrence	Detectability	Severity						

Vita

Major Charlie Middleton is an active-duty officer in the U.S. Air Force, currently stationed at Wright-Patterson Air Force Base at the Air Force Institute of Technology. Major Middleton is a fighter pilot, primarily in the F-16 Fighting Falcon. He has over two thousand flight hours as pilot in command of military aircraft and over 500 flight hours of instructor pilot time in the F-16. He is a combat veteran, having served in Operation Southern Watch in Saudi Arabia and Iraq in 2002, and in Operation Iraqi Freedom in Iraq in 2003 and 2005. He flew an F-16 Suppression of Enemy Air Defenses mission in the first daylight strike on Baghdad in the Iraq War. He was the top graduate of his F-16 training class, and has been awarded a variety of other awards, medals, and military decorations.

Major Middleton is also a Test Pilot, having graduated as a Distinguished Graduate of the U.S. Naval Test Pilot School in 2009. He has recently flown flight test missions which explore and evaluate current and developing weapons systems, including tests of next-generation bombs, missiles, bullets, radars, targeting systems, and other aircraft systems.

Prior to joining the Air Force, Charlie was a Summa Cum Laude graduate of Princeton University with a Bachelor of Science in Engineering degree in Operations Research, and a Certificate in Management Systems. Charlie is a graduate of Carroll High School in Dayton, Ohio. He was the class of 1994's Valedictorian, Athlete of the Year, and Patriot of the Year.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
14-06-2012	Master's Graduate Research Paper	Jun 2011 – Jun 2012

4. TITLE AND SUBTITLE

Risk Assessment Planning for Airborne Systems: An Information Assurance Failure Mode, Effects and Criticality Analysis Methodology

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Middleton, Charles J., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Street, Building 642
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/IOA/ENS/12-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ASC/EN Attn: Dr. Raju B. Patel
2145 Monahan Way
Wright Patterson AFB, Ohio 45433-7017
e-mail: kalabhai.patel@wpafb.af.mil DSN: 785-9566

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Increasingly in recent times, aircraft are built with communications links to external participants. These communications links may in some cases be susceptible to degradation or attack, which may then lead to safety of flight or mission effectiveness risks. This project examines risk assessment of the information assurance and security of newly developed airborne systems. First, an investigation of the past failures of the security of other networked systems is examined, to give a historical perspective on the likely scope of system security threats and vulnerabilities. Next, risk assessment methods are summarized for current methods of analyzing risk to aircraft and other systems. An information assurance Failure Mode, Effects and Criticality Analysis (FMECA) methodology is presented, based on past FMECA methodologies with modifications tailored to aircraft systems and the information warfare environment, to examine the system integrity considerations in planning for the development of new military aircraft. A program manager's potential decisions are informed with insights on failure mode risk criticality, based on the information assurance FMECA method. Finally, recommendations for follow-on research in the airborne systems information assurance field are detailed.

15. SUBJECT TERMS

Risk Assessment, Criticality, Failure Mode, Information Assurance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Raymond R. Hill, PhD
U	**U**	**U**	**UU**	65	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636; e-mail: Raymond.Hill@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18